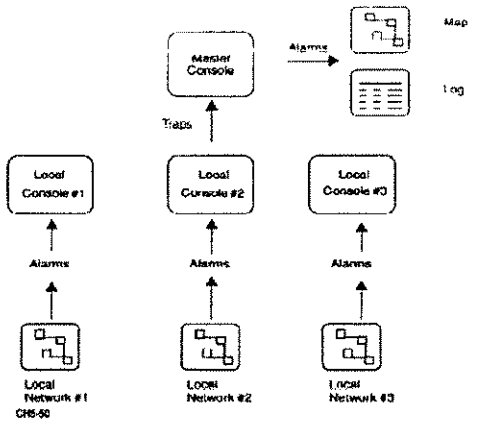
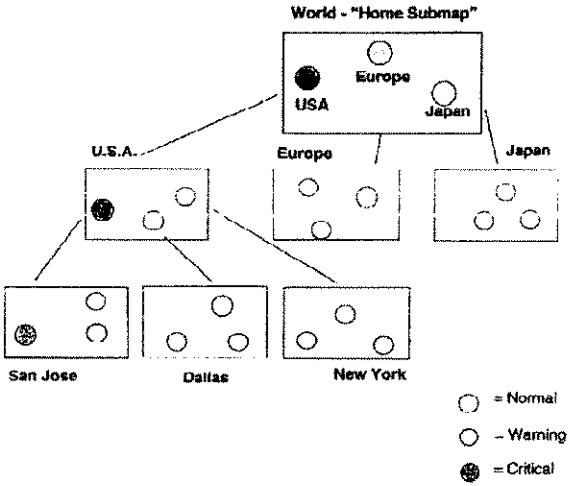
HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Alarm Forwarding Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console. Selected alarms at the local console can be converted to traps and sent to another console." (4-28) [SYM_P_0081026]  (4-28) [SYM_P_0081026] --- See Figure 13 in my expert report.

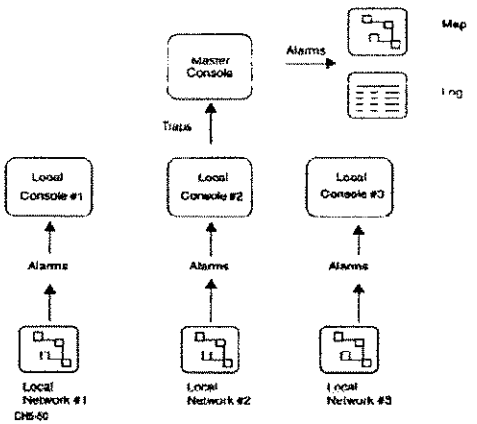
HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
8	The method of claim 7, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	"Before you create a network map, you need to know the physical layout of your network. If may be a single LAN, several LANs, or a very complex enterprise-wide network. Whenever possible you should break your map into submaps that help you visualize the network organization. You can create submaps for a workgroup, building site, device type, or any other convenient grouping. The same device can be placed on several submaps to provide alternate "views" of the network. … The submap symbol displays the most severe status color for all of the nodes or devices within it. This allows the most severe status information for any device in the network to be propagated up to the home submap. The home submap can then give you an overview of status for the entire network." (3-2) [SYM_P_0080984] "**Alarm Database** Every alarm is recorded in an alarm database. Each entry contains the date and time, status, device name, and device type of the alarm." (4-31) [SYM_P_0081029]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		 "Figure 4-2 Map set to propagate alarms up all levels." "Normally, you would select to propagate up all levels. Then, if your home submap contains a submap symbol for each submap in the next lower level in the map, you can check your network's overall status from the home submap. If a submap represents several devices, its submap symbol on the home submap will display the most severe device status for the lower submap." (4-19) [SYM_P_0081017]

HP OpenView for Windows User Guide
"HP OpenView"

'203' Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Alarm Forwarding Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console. Selected alarms at the local console can be converted to traps and sent to another console." (4-28) [SYM_P_0081026]  (4-28) [SYM_P_0081026] --- See Figure 13 in my expert report.

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
9	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 8 See Figure 13 in my expert report.
10	The method of claim 9, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 8 **"Alarm Forwarding** Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console." (4-28) [SYM_P_0081026]
11	The method of claim 9, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	"**Alarm System** OpenView allows you to configure how alarms will be processed or displayed on maps, clear alarm conditions, and create reports from the alarm log. In addition, you can configure alarms of a particular level to start programs, send pages, or be forwarded to other workstations." (1-6) [SYM_P_0080962]
12	An enterprise network monitoring system comprising:	See '203 claim 1

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
	a plurality of network monitors deployed within an enterprise network;	See '203 claim 1
	said plurality of network monitors detecting suspicious network activity	See '203 claim 1
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	See '203 claim 1
	said network monitors generating reports of said suspicious activity; and	See '203 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and	See '203 claim 1

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
	integrate the reports of suspicious activity.	
13	The system of claim 12, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
14	The system of claim 12, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
15	The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
16	The system of claim 12, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
17	The system of claim 12, wherein the network	See '203 claim 6

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
	monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	
18	The system of claim 12, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8
19	The system of claim 18, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8
20	The system of claim 12, wherein the plurality of network monitors include a plurality of domain	See '203 claim 9

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
	monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	
21	The system of claim 20, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10
22	The system of claim 20, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '203 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1
2	The method of claim 1, wherein integrating	See '203 claim 2

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
	comprises correlating intrusion reports reflecting underlying commonalities.	
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information: ... The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966] "Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958] "The **Component** symbol set contains various network components such as hubs, routers, and multiplexers.

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
		OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996] --- See Figure 13 in my expert report. "Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111] "Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered: 1.3.6.1.4.1.42 The "Flintstones, Inc." enterprise might then register their "Fred Router" under the name of: 1.3.6.1.4.1.42.1.1" (RFC 1155 p. 6) [SYM_P_0501017] "See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
		standard." (RFC 1155 p. 1) [SYM_P_0501013] "sysServices OBJECT-TYPE . . . ' . . . layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays) For systems including OSI protocols, layers 5 and 6 may also be counted.'" (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156] "ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1), -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }" (RFC 1213 p. 25) [SYM_P_0501165] "Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices ... An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208]

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
7	The method of claim 1, wherein at least one of said network monitors utilizes a statistical detection method.	**103:** *See* Feather, Frank Edward, Ph.D., "Fault Detection in an Ethernet network via anomaly detectors", Carnegie Mellon University, Order number 9224199, 1992 [SYM_P_0501779- SYM_P_0502036].
8	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
9	The method of claim 8, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8
10	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
11	The method of claim 10, wherein receiving and integrating is performed by an enterprise	See '203 claim 10

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
	monitor with respect to a plurality of domain monitors within the enterprise network.	
12	The method of claim 10, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11
13	An enterprise network monitoring system comprising:	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network,	See '615 claim 1
	said plurality of network monitors detecting suspicious network activity	See '615 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '615 claim 1
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1
	one or more hierarchical monitors in the	See '615 claim 1

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
	enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	
14	The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2
15	The system of claim 13, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
16	The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4
17	The system of claim 13, wherein the enterprise network is a TCP/IP network.	See '203 claim 5
18	The system of claim 13, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '615 claim 6
19	The system of claim 13, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7
20	The system of claim 19, wherein a domain monitor associated with the plurality of service	See '203 claim 8

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
	monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	
21	The system of claim 13, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9
22	The system of claim 21, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10
23	The system of claim 21, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11
34	A computer-automated method of hierarchical even monitoring and analysis within an enterprise network comprising:	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a gateway;	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information: ... The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966]

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958] "The **Component** symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996] --- See Figure 13 in my expert report. "Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p. 4) [SYM_P_0527111] "Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in management protocols. For example, if the

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered: 1.3.6.1.4.1.42 The "Flintstones, Inc." enterprise might then register their "Fred Router" under the name of: 1.3.6.1.4.1.42.1.1" (RFC 1155 p. 6) [SYM_P_0501017] "See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard." (RFC 1155 p. 1) [SYM_P_0501013] "sysServices OBJECT-TYPE . . . ' . . . layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays) For systems including OSI protocols, layers 5 and 6 may also be counted.'" (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156] "ipForwarding OBJECT-TYPE SYNTAX INTEGER {

HP OpenView for Windows User Guide
"HP OpenView"

'615 Claim number	Claim Term	HP OpenView (printed publication and public use)
		forwarding(1), -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }" (RFC 1213 p. 25) [SYM_P_0501165] "Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices … An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208]
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1
35	The method of claim 34, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See'203 claim 2
36	The method of claim 34, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3
37	The method of claim 34, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4